COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2020
Preventing a 'code red' with an effective supplier code of conduct

By Steve Hager andCris Mattoon, JD, CCEP, CAMS, MCM

Steve Hager (srhager@autoclubgroup.aaa.com) is Ethics Program Manager at The Auto Club Group in Dearborn, Michigan, USA. **Cris Mattoon** (cqmattoon@autoclubgroup.aaa.com) is Assistant Vice President, Compliance & Ethics, at The Auto Club Group, and Chief Bank Compliance Officer, at Auto Club Trust FSB in Dearborn, Michigan, USA.

Outsourcing and co-sourcing are no longer the exception to the rule, but are key to effective resource management in today's economy. No longer solely the province of large corporations, organizations of all sizes across industries employ vendors, contractors, and consultants to perform core functions. Although the upside of using external resources often results in greater financial and operational efficiency and improved customer outcomes, boards of directors and CEOs must ensure that adequate safeguards are implemented to mitigate risk. An effective supplier code of conduct should be central to such measures.

A pillar of prudent risk management

Business conduct may no longer be left to chance. It seems that a shocking news story emerges daily due to some cybersecurity incident, harassment, discrimination, or physical injury associated with a well-known brand. Like a forest fire leaping the fire control line, these stories leap from cable news onto social media where the conflagration goes global in the blink of an eye. What often escapes the initial spread of the negative news story is the role that a supplier may have played in the unfortunate incident.

Think Target Corporation and its HVAC vendor,[1] whose own allegedly inadequate risk management practices allowed hackers to steal a reported 40 million credit card numbers in one of the biggest data breaches in history. Although almost no one informed of the incident and its subsequent litigation could name the HVAC vendor, practically everyone associates the breach with the red bullseye logo. Your board of directors doesn't want to find itself at the center of a litigator's or regulator's costly and embarrassingly public "bullseye."

In addition to ongoing supplier due diligence, legally binding contracts, and sufficient insurance coverage, supplier codes of conduct provide a key pillar of prudent risk management. A vibrant *employee* code of conduct, frequently discussed at all levels of an organization and among employees, can mitigate inappropriate and unethical internal behavior. Likewise, a *supplier* code of conduct, carefully tailored to the industry and reflective of mutual expectations between the contracting organization and its vendors, contractors, and consultants can guide third-party behavior before it reflects badly upon your brand.

Tailoring the code to suppliers

Codes of conduct are not one size fits all. Thus, it's not simply a matter of rebranding your employee code of conduct with a new "supplier" title. Although comprehensive employee codes of conduct may cover a gamut of relevant legal, regulatory, and ethical topics supportive of the organization's internal culture and reflective of the employer/employee relationship, the supplier code must adhere more narrowly to the topics germane to the arm's-length relationship enjoyed between the organization and its third-party suppliers.

One approach has been to draft an entirely new document tilted toward that supplier relationship. Forward-looking chief ethics and compliance officers (CECOs) are realizing that there are key areas of commonality between the code topics observed by employees and those observed by suppliers. Bribery, money laundering, discrimination, and misuse of customer information are just a few examples of such legal, regulatory, and ethical obligations owed by both employees and suppliers toward your organization.

Engage appropriate internal business partners involved in your organization's sourcing process to identify pertinent topics to retain from your employee code, and additional topics that reflect the unique aspects of third-party relationships. At a minimum, I recommend including your legal, internal audit, procurement, information security, and loss prevention peers in this exercise. Although the final verbiage will necessarily need to be revised to reflect the supplier (versus employee) relationship that your organization maintains with the third party, the majority of the content will remain relevant as you draft your supplier code.

Aligning the code with the procurement process

Beyond engaging your internal peers to identify relevant supplier-centric topics to include in the code, you also will seek their input throughout the implementation process to ensure that the supplier code aligns with each phase of the procurement process from the request for proposal through contract renewals. As the CECO, your involvement in sourcing suppliers is likely limited to specific aspects of precontract or ongoing due diligence, as well as investigations of alleged incidents reported through the hotline.

Your legal partner will ensure that the master services agreement and statements of work contemplate the presence of and bind the third party to observe the terms of the supplier code of conduct. Your information security partner will provide expertise regarding the current nature of regulatory and industry standards for which third parties are expected to abide to protect company and consumer confidential information. Procurement, loss prevention, and internal audit partners will provide insights that reflect red flags identified during prior similar engagements or across the industry, for which an effective code of conduct can mitigate future risk to your organization. As they say, "It takes a village."

Suppliers as trusted partners

The forgoing guidance is not meant to imply that vendors, contractors, and consultants are untrustworthy or careless as a general rule. In fact, your suppliers are trusted partners who your organization has contracted to expand your capacity to best serve your customers and operate with efficiency. But as Arthur Andersen[2] learned nearly two decades ago, sometimes it only takes one unethical business partner to irreparably harm an otherwise sound organization. In a global economy beset by class-action litigation and regulated across borders by domestic and international agencies with sometimes-divergent enforcement missions, it is incumbent upon an ethically responsible and law-abiding organization to hold its suppliers to a predictable, well-grounded set of standards in advance of and throughout the duration of their mutual relationship.

Conclusion

Suppliers are vital strategic business partners to organizations large and small. Mitigating the risks inherent in such third-party relationships protects customers, employees, boards of directors, and the assets of the organization. Much like a personal reputation, failure to put appropriate safeguards in place—especially an effective supplier code of conduct—to protect your brand can result in irreparable harm to your organization. Collaborate with key internal business partners to craft and communicate a tailored code of conduct to your suppliers to achieve the best outcome for all parties.

Takeaways

- Beyond the employer/employee relationship, codes of conduct are an effective risk management tool for supplier relationships.
- A supplier code reduces foreseeable risks to your organization, your customers, and your employees.
- Engaging key internal partners—legal, internal audit, loss prevention, procurement, and information security—will ensure that your supplier code reflects the holistic risks involved in third-party relationships.
- Trusted partnerships with vendors, contractors, and consultants are strengthened when the legal, regulatory, and ethical expectations are uniformly documented and shared in advance of contracting.
- Litigators and regulators expect that organizations will exercise the foresight to hold suppliers to acceptable and enforceable standards of business conduct.

1 Kevin McCoy, "Target to pay $18.5M for 2013 data breach that affected 41 million consumers," *USA Today*, last modified May 23, 2017, http://bit.ly/2MLSbwX.
2 Flynn McRoberts, "The fall of Andersen," *Chicago Tribune*, last modified September 1, 2002, http://bit.ly/2FgxXHy.